Remarks

The present response is to the Office Action mailed in the above referenced case on March 23, 2005. Claims 1- 28 are pending in the application. Claims 1-9, 14-22, 26 and 27 are rejected under 102(e) as being anticipated by Sweet et al. (US Pub 2002/0031230). Claims 1, 10, and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by Lincke et al. (US 6,253,326) hereinafter Lincke. Claims 11, 12, 23-25 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet in view of Lincke.

Applicant has carefully reviewed the prior art references provided by the Examiner, and the Examiner's statements and rejections of the instant Office Action. In response applicant presents new claims 29-48 for examination. Claims 1-28 are canceled.

Applicant herein provides newly written independent claims 29 and 39 for examination. The new claims positively recite creating a VPN tunnel in the Internet, which adds security to the wireless database management system.

In the presently preferred embodiment of the wireless database management system (WDMS), it is possible for a virtual private network (VPN) to provide additional security to data transferred between a VPN client 5 in FIG.1 and a VPN Intranet 160. FIG. 3 shows an embodiment of the detailed structure of a VPN client 5, and FIG. 5 shows an embodiment of the detailed structure of a VPN Intranet. A VPN is implemented by limiting access to every computer or computer network intervening a wireless base station 30 in FIG. 3 and a web or application server 90 in FIG. 5.

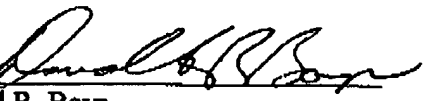
As illustrated in applicant's specification, the main differences in the structure of a typical client as shown in FIG. 2 and a VPN client as shown in FIG. 3 are the VPN-controlled wireless proxy server 60 in FIG. 3 and the VPN Tunnel 75. A wireless base station 30 might connect to a VPN-controlled wireless proxy server 60 rather than a standard wireless proxy server (50 in FIG. 2). The VPN-controlled wireless proxy server might then connect to only certain VPN-controlled servers that are also connected to the

Internet. The plurality of VPN-controlled Internet servers between a VPN-controlled proxy server 60 and a web or application server 90 in FIG. 5 is known as a VPN Tunnel 75. Similarly, the main difference in the structure of a typical Intranet as shown in FIG. 4 and a VPN Intranet as shown in FIG. 5 is the VPN Tunnel 75. In this embodiment, the VPN does not allow users outside the WDMS to have any access to data transferred within the WDMS; they cannot inspect data within the WDMS and they cannot find out from whence data is transmitted or received — they cannot see the data at all.

Applicant believes that providing a VPN tunnel in the Internet to transfer data between a wireless device and information from a database in a WDMS is certainly novel in the art.

In view of applicant's newly presented claims, the Examiner's present rejections are moot. As all of the newly presented claims standing for examination are novel and clearly patentable over the art of record, applicant respectfully requests reconsideration, and that the present case be passed quickly to issue. If there are any time extensions needed beyond any extension specifically requested with this response, such extension of time is hereby requested. If there are any fees due beyond any fees paid with this amendment, authorization is given to deduct such fees from deposit account 50-0534.

Respectfully Submitted,
Ari D. Kaplan

by 
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency
P.O. Box 187
Aromas, CA 95004
(831) 726-1457